BLACK DUCK®



Cobham Satcom Automates Application Security with Black Duck

ABOUT COBHAM SATCOM

Industry: Aerospace, Defense, and Maritime Technology

Headquarters: Denmark (with U.S. operations)

Core business area

Satellite communications terminals for maritime and land use

Challenge

Application security that meets the scale, complexity, and accuracy requirements of maritime and MilGov customers

Requirements

- High-accuracy scanning to support mission-critical applications
- Comprehensive code scans for software with a 30-year life cycle
- Integration with CI/CD pipeline to minimize human intervention
- Static analysis with deep C and C++ support, including call flow analysis
- Software composition analysis with signature scanning
- Support for legacy platforms like RHEL 6

Solutions

- Black Duck SCA
- Coverity Static Analysis

Cobham Satcom develops advanced radio and satellite connectivity solutions for high-stakes operations on land and at sea.

Designed for the world's most demanding environments, the company's precision-engineered technology delivers the performance and resilience required to keep critical communications running. Trusted across maritime, government, and enterprise sectors, Cobham Satcom plays a key role in ensuring reliable connectivity where safety, mission success, and business continuity depend on it.

With an evolving codebase and increasing regulatory demands, the challenge was not introducing security controls, but ensuring that they could be applied consistently, at scale, and without slowing development down.

Shortly after strengthening its cybersecurity leadership, Cobham Satcom focused on standardizing and expanding existing capabilities. It integrated Coverity® Static Analysis and Black Duck® SCA into its CI/CD pipeline to help ensure that application security could operate as part of engineering, rather than alongside it.

THE CHALLENGE: Making application security scale in practice

Cobham Satcom builds and maintains embedded Linux software across both modern and legacy platforms. The majority of the codebase is written in C and C++, but it also includes modern codebases on top, with development distributed across teams in Denmark (Bitbucket) and the U.S. (GitLab).

The challenge was not the absence of tooling but rather ensuring it worked consistently across the organization. "Given how the codebase has evolved over time—across platforms, teams, and technologies—manual review and validation weren't viable," said Lemuel Valdez, chief information security officer (CISO) at Cobham Satcom. "We either had to automate or accept gaps."

At the same time, expectations around software security continued to increase. "There are more requirements around how software is developed and maintained over its lifetime," Valdez said. "You need to be able to demonstrate control continuously, not just at release. If it depends on manual intervention to hold together, it won't scale. And if it doesn't scale, it doesn't give you control."

> **"Given how the codebase has evolved over time—across platforms, teams, and technologies—manual review and validation weren't viable."**
>
> —Lemuel Valdez, CISO, Cobham Satcom

An evolving regulatory and operating context

Frameworks such as ISO 27001 and requirements like the NIS2 Directive are raising expectations around accountability, traceability, and life cycle management. This introduced a variety of practical requirements.

- Consistent scanning across C/C++ environments
- Coverage of both proprietary and third-party components
- Integration into CI/CD pipelines
- Minimal reliance on manual validation
- Support for legacy platforms alongside modern environments

THE SOLUTION: Coverity Static Analysis and Black Duck SCA

Cobham Satcom evaluated several tools, focusing on how they perform in real-world conditions rather than feature comparisons. "The deciding factor was how well the tools handled C and how much we could trust the results," Valdez said. "If the signal isn't reliable, you end up compensating with manual work."

Deployment flexibility was also an important factor. "We operate across different customer environments and regulated contexts, where requirements can vary," Valdez said. "The tooling needs to work within those constraints, not the other way around."

Rather than standardizing on a single deployment model, Cobham Satcom prioritized solutions that could operate across controlled environments, including on-premises setups where tight integrations with existing tooling are required. "Security comes first," Valdez said. "You have to be able to run the platform in a way that aligns with where and how you operate."

Coverity provides deep static analysis, including call flow and execution path awareness, enabling more precise identification of issues. "Most tools will flag a large number of potential issues," said Mathias Mortensen, lead DevOps engineer at Cobham Satcom. "If you still need to work out which ones actually matter, you haven't really reduced the effort."

Black Duck SCA provides improved visibility, particularly in embedded environments, for open source and third-party components. "In environments like Yocto or Buildroot, you're often working with components that aren't fully visible through package managers," Mortensen said. "You need to understand what's actually in your codebase, not just what's declared." Black Duck SCA's signature scanning and KnowledgeBase™ provide that level of insight and accuracy.

> **"Most tools will flag a large number of potential issues, If you still need to work out which ones actually matter, you haven't really reduced the effort."**
>
> —Mathias Mortensen, DevOps Engineer, Cobham Satcom

Rapid integration with the right partners

The capabilities provided by the Black Duck solutions were not entirely new, but the approach to integrating and scaling them was. "The priority was to bring everything together and make it work consistently," Valdez said.

With support from Eficode, as well as internal and Black Duck teams, Cobham Satcom was able to integrate and operationalize application security across its environments within a short timeframe. "It wasn't about starting from scratch," Valdez said. "It was about aligning what we had and making it work properly end-to-end."

THE RESULTS: Consistent execution with less friction

The primary outcome was not just improved detection, but consistent and repeatable execution of application security within the software development life cycle. By integrating Coverity and Black Duck into its CI/CD pipelines, Cobham Satcom now ensures that

- Scanning runs automatically on each build
- Findings are identified directly within developer workflows
- Thresholds enforce risk tolerance without manual gates

"The objective wasn't to add another step," Valdez said. "It was to make security part of how builds run."

Improved accuracy and usability

Valdez notes that the main improvement was in the quality and usability of results. "What we saw was an improvement in how accurately vulnerabilities were identified across both internal and third-party components. That gave us a much clearer picture of what actually needs attention, he said. "It's not just about scanning more often—it's about being confident that what you're seeing is relevant and complete enough to act on."

"The objective wasn't to add another step. It was to make security part of how builds run."

—Lemuel Valdez, CISO, Cobham Satcom

Reduced manual overhead without losing control

That accuracy translated directly into efficiency. "If the output isn't reliable, you compensate with manual verification," Valdez said. "That quickly becomes the bottleneck—and then you lose both speed and control." With more trusted results, the team found that

- Developers spend less time validating findings
- Security teams are not required to intervene manually
- Development flow continues without unnecessary disruption

"I'd rather have the pipeline enforce the rules than us stepping in and blocking things manually," Valdez said.

LOOKING AHEAD: Scaling with AI, NIS2, and increasing expectations

Cobham Satcom continues to evolve its approach as development becomes faster and more complex, particularly with AI-assisted development and increasing regulatory expectations. The focus remains on strengthening the foundation.

- Trusted and accurate security data
- Consistent execution through pipelines
- Integration across development, security, and risk

"AI will increase both the speed and volume of software development," Valdez said. "That means more code, more dependencies, and more potential exposure. If the control model doesn't scale with that, it breaks."

At the same time, expectations are shifting. "With NIS2 and similar frameworks, it's becoming less acceptable to treat vulnerabilities as something you fix later," Valdez said. "There is an expectation that you control what you release, not just how you respond afterward."

From Cobham Satcom's perspective, this is both a regulatory and engineering principle. "We don't want to ship something that introduces avoidable risk into environments outside our control," Valdez said. "That needs to be addressed before release, not after."

Maintaining developer flow remains a key requirement, as well. "If you overburden developers, they will bypass the system," said Mortensen. "The goal is to automate and embed, so security happens without getting in the way."

As visibility improves, the number of identified vulnerabilities is expected to increase. "Higher visibility naturally leads to more findings," Valdez said. "That's why accuracy and prioritization become more important over time."

Cobham Satcom is also progressing toward becoming a CVE Naming Authority (CNA), reflecting a more proactive role in vulnerability management. "Becoming a CNA is a natural step when you move from consuming vulnerability data to actively managing it," Valdez said. "That requires confidence in what you see and how you act on it."

"The tools matter—but only because they fit into how we operate," Valdez said. "That's what allows us to move forward without increasing risk or slowing down the people building the systems."

"The goal is to automate and embed, so security happens without getting in the way."

—Mathias Mortensen, DevOps Engineer, Cobham Satcom

SUMMARY

By integrating Coverity and Black Duck into its development pipelines, Cobham Satcom established a practical and scalable approach to application security. Security is now

- Automated and consistently executed
- Embedded directly into development workflows
- Based on results that teams can trust and act on

This enables Cobham Satcom to balance

- Long-lived, complex systems
- Increasing regulatory expectations
- Faster development driven by modern practices and AI

Application security operates as part of the system, supporting the organization's ability to evolve without adding friction or losing control.

About Black Duck

Black Duck® meets the board-level risks of modern software with True Scale Application Security, ensuring uncompromised trust in software for the regulated, AI-powered world. Only Black Duck solutions free organizations from tradeoffs between speed, accuracy, and compliance at scale while eliminating security, regulatory, and licensing risks. Whether in the cloud or on premises, Black Duck is the only choice for securing mission-critical software everywhere code happens. With Black Duck, security leaders can make smarter decisions and unleash business innovation with confidence. Learn more at www.blackduck.com.

©2026 Black Duck Software, Inc. All rights reserved. Black Duck is a trademark of Black Duck Software, Inc. in the United States and other countries. All other names mentioned herein are trademarks or registered trademarks of their respective owners. September 2026